

법률(근거법령)	행정규칙 (최종 개정일 / 시행일)	법령 위계	세부내용	해당 솔루션						패널티
				SpamSniper	MailScreen	JVault+	OfficeHard	MobileKeeper	MailSafer	
개인정보보호법	개인정보보호법 (*16.03 / *16.09)	특별 법률	제3조 개인정보보호 원칙 / 개인정보 안전한 관리		○		○		○	- 주민등록번호 분실, 도난, 유출, 위조, 변조, 훼손 방지 위한 안전성 확보 조치 필수 - 개인정보보호 법규 위반행위시(개인정보 미파기시, 암호화 조치 미이행시, 안전성 확보 조치 미이행시 등) 3천만원 혹은 5천만원 이하의 과태료 부과 - 개인정보처리자의 고의 또는 과실로 개인정보 분실·도난·유출·위조·변조·훼손시 300만원 이하 손해액 배상 청구 가능 (*제39조의2 개인정보 주의, 감독 책임 개월러하지 아니한 경우 손해배상책임 경감* 항목 삭제) - 개인정보보호 법규 위반행위시 경계 권고 대상에 대표자 및 임원 포함
			제23조 민감정보(성상, 신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등)의 분실, 도난, 유출, 위조, 변조, 훼손 방지 위한 안전성 확보 조치 필수		○		○		○	
			제24조 고유식별정보(주민등록번호, 여권번호, 운전면허번호, 외국인등록번호)의 분실, 도난, 유출, 위조, 변조, 훼손 방지 위한 안전성 확보 조치 필수 / 개인정보 종류, 규모, 중요원수, 매출규모 등에 따라 안전성 확보 조치 정기조사		○		○		○	
			제24조의2 법령으로 지정된 경우 제외 주민등록번호 처리 금지 / 주민번호 처리 불가피한 경우 분실, 도난, 유출, 위조, 변조, 훼손 방지 위한 암호화 필수 (주민번호 100만건 미만 : 2017년부터, 100만건 이상 : 2018년부터)		○		○		○	
			제29조 개인정보 분실·도난·유출·위조·변조·훼손 방지 위한 내부 관리계획 수립, 접속기록 보관 등 안전성 확보에 필요한 기술적·관리적 및 물리적 조치 필수		○		○		○	
	표준 개인정보 보호지침 (*16.06 / *16.06)	고시	제4조 개인정보 처리시 관리적·기술적 및 물리적 보호조치를 통해 개인정보 안전 관리	○	○	○	○	○	○	
			제10조 개인정보 보유기간 경과 및 처리목적 달성, 서비스 및 사업 종료 등 개인정보 불필요하게 되었을 경우 정당한 사유 없는 한 5일 이내 개인정보 파기		○		○		○	
			제11조 개인정보 파기하지 않고 보존해야하는 경우 물리적 또는 기술적 방법으로 분리·저장 관리		○		○		○	
	개인정보의 안전성 확보조치 기준 (*16.09 / *16.09)	고시	제15조 개인정보취급자 최소한 지정 및 개인정보 처리 범위 최소한의 범위로 제한 및 차등 부여, 접근권한 관리 조치		○		○		○	
			제3조 개인정보의 안전성 확보 조치시 '개인정보처리자 유형 및 개인정보 보유량에 따른 기준 적용' - 유형1(완전) : 개인정보 1만명 미만 보유한 소상공인, 단체, 개인 - 유형2(표준) : 개인정보 100만명 미만의 보유한 중소기업 / 10만명 미만의 보유한 대기업, 중견기업, 공공기관 / 1만명 이상 보유한 소상공인, 단체, 개인 - 유형3(강화) : 개인정보 10만명 이상 보유한 대기업, 중견기업, 공공기관 / 100만명 이상 보유한 중소기업, 단체	○	○	○	○	○	○	
제4조 개인정보 분실, 도난, 유출, 위조, 변조, 훼손 방지를 위한 15개 조항에 대한 내부 관리계획 수립, 시행 의무 △개인정보 보호책임자 지정 △개인정보 보호책임자 및 개인정보취급자의 역할 및 책임 △개인정보취급자 교육 △접근 통제에 관한 사항 △개인정보 암호화 조치 △접속기록 보관 및 점검 △악성프로그램 등 방지 △물리적 안전조치 △개인정보 보호조치에 관한 구성 및 운영 △개인정보 유출사고 대응 계획 수립·시행 △위험도 분석 및 대응방안 마련 △재해 및 재난 대비 개인정보처리시스템의 물리적 안전조치 △개인정보 처리업무 수탁자에 대한 관리 및 감독 △기타 필요 사항				○		○		○		
제6조 개인정보 유출 방지 위한 모바일 기기 접근제어 및 분실, 도난 등에 대한 비밀번호 설정 등 보호조치				○		○		○		
제7조 개인정보 정보통신망, 보조저장매체 통한 송수신시 암호화 / DMZ 영역 및 모바일기기에 개인정보 저장시 암호화				○		○		○		
정보통신망법	정보통신망 이용촉진 및 정보보호 등에 관한 법률 (*16.03 / *16.09)	특별 법률	제28조 개인정보 내부관리계획의 수립·시행 / 접속기록 위·변조 방지 / 개인정보 보안 저장·전송 위한 암호화 기술 등	○	○	○	○			
			제29조 정보통신서비스 1년간 미사용 이용자 개인정보 파기		○		○			
			제48조의4 정보통신망의 접속기록 등 관련 자료 보존	○	○	○	○			
	개인정보의 기술적·관리적 보호조치 기준 (*15.05 / *15.05)	고시	제4조 개인정보 접근권한 제한, 불법유출, 다운로드, 파기 금지 / 개인정보취급자 컴퓨터 망분리 의무 / 정보통신서비스 제공자 컴퓨터, 모바일 기기 대상 정보유출 방지 조치	○	○	○	○	○	○	
			제5조 개인정보취급자 접속기록 확인, 보존, 관리 / 개인정보취급자 접속기록 위변조 방지, 별도 저장, 정기 백업 실시		○		○		○	
			제6조 고유식별정보, 신용카드번호, 바이오정보 암호화 / 개인정보 송수신시 보안서버 구축 / 컴퓨터, 모바일 기기 등 저장시 암호화		○		○		○	
			제7조 백신SW 자동 업데이트 및 일 1회 이상 업데이트 / 악성프로그램 발생시 또는 해당 SW 보안 업데이트 공지가 최신SW 업데이트 실시	○	○	○				
	(개인)정보보호 관리체계 인증 등에 관한 고시 (*16.06 / *16.06)	고시	보호대책요구사항) 모바일 기기접근 통제 / 모바일기기 반출입				○		○	
			보호대책요구사항) 개인정보 취급자 지정 및 감독 / 개인정보 보호 서약				○		○	
			보호대책요구사항) 개인정보처리시스템 접근 권한 관리 / 접속 기록 저장 / 위변조 방지				○		○	
전자금융거래법	전자금융거래법 (*16.01 / *16.07)	특별 법률	제9조 접근매체 위변조 및 정보통신망 침입 등을 통한 사고 발생시 금융회사 또는 전자금융업자 책임	○	○	○	○			
			제21조 전자금융거래의 안전성 확보 / 전자금융업무에 대한 금융위 기준 준수 및 매년 정보기술부문 계획 금융위 제출	○	○	○	○	○	○	
			제21조의4 접근권한 제한 및 권한 외 데이터 조작, 파괴, 은닉, 유출 등 행위 금지		○		○		○	
			제22조 금융회사 전자금융거래기록 최대 5년 보존 (추적, 검색, 오류 확인용) / 기간경과 및 상거래관계 종료시 5년 이내 파기		○		○		○	
	전자금융 감독규정 (*16.10 / *16.10)	고시	제8조 정보기술부문 인력은 임직원의 5% 이상, 정보보호인력은 정보기술부문 인력의 5% 이상, 정보보호예산 정보기술부문의 7% 이상이 되도록 할 것	○	○	○	○	○	○	
			제12조 담당자 외 단말기 무단조작 금지 / 사용자 인증 기록 유지 / 외부반출, 인터넷접속, 그룹웨어접속 금지 단말기 지정 / 보조기억매체 및 휴대용 전산장비 접근 통제		○		○		○	
			제13조 접근권한 제한 / 전산자료, 장비 반출입 통제 / 가동기록 1년 이상 보존 / 5회 접속오류시 차단 / 단말기 이용 제한	○	○	○	○	○	○	
			제15조 해킹 등 방지시스템 운영 / 프로그램 패치 즉각 반영 / 인터넷-업무망 분리, 차단 (단, 업무상 필수적으로 특정 외부기관과 연결해야하는 경우 제외)	○	○	○	○		○	
			제16조 악성코드 감염 방지대책 수립, 운용	○	○	○			○	
			제18조 직무 특성별 네트워크 분리 및 IP 주소 사용, 외부직원 공동작업 등 네트워크 분리 어려울 경우 IP주소 접근권한 분리		○		○		○	
클라우드발전법	클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 (*15.03 / *15.09)	특별 법률	제5조 주요 행정기관 클라우드컴퓨팅 관련 기본계획 3년마다 수립, 매년 시행계획 수립 및 시행	○	○	○	○			
			제12조 국가기관의 국가정보화 정책 및 사업 예산 편성시 클라우드컴퓨팅 도입 우선 고려	○	○	○	○			
			제13조 국가기관 연1회 이상 소관기관 클라우드컴퓨팅 사업 수요정보 제출	○	○	○	○			
			제20조 정부의 공공기관 클라우드컴퓨팅서비스 이용 촉진	○	○	○	○			
	공공기관 민간 클라우드 이용 가이드라인 (*16.07 / *16.07)	가이드라인	민간 클라우드 이용 기준 및 절차 : 민간 클라우드 이용 가능 여부 자체 검토(국정원 '국가 공공기관 클라우드컴퓨팅 보안 가이드라인' 준수 및 인증 받은 서비스 이용) 계약서 작성 : 공공기관용 표준계약서와 서비스수준협약서(SLA) 참고하여 계약 체결	○	○	○	○			
정보보호산업진흥법	정보보호산업의 진흥에 관한 법률 (*15.06 / *15.12)	특별 법률	제3조 국가 및 지방자치단체 정보보호산업 진흥 정책 수립 및 시행, 재원확보 방안 마련 책무	○	○	○	○	○	○	
			제6조 행정/공공기관 매년 정보보호기술 등에 대한 구매수요정보 제출 및 구매수요정보 정보보호기업에 제공	○	○	○	○	○	○	
			제7조 정보보호제품 및 정보보호서비스에 대한 적정 수준 대가 지급	○	○	○	○	○	○	
			제12조 정보통신서비스 제공/매개자 대상 정보보호준비도 평가 지원	○	○	○	○	○	○	
			제13조 정보통신서비스 제공/매개자 정보보호 투자 및 인력 현황, 정보보호 관련 인증 등 정보보호 현황 공개	○	○	○	○	○	○	
			제23조 정보보호 전문서비스 기업 지정 및 관리	○	○	○	○	○	○	
	SW사업 대가산정 가이드 (*16.06/06.06)	가이드라인	보안성 지속 서비스비 산정시 (최초 제품 구매 계약 금액 X 서비스 요율) 기준 별도 산정	○	○	○	○	○	○	
모바일보안 솔루션 도입시 필수 요구사항		공공기관 스마트폰 보안 규정 (국정원) 스마트워크 정보보호 가이드라인 (금감원) 모바일 정보보호 가이드라인(금감원)						MOBILEKEEPER 모바일 키퍼		

기업·조직 규모 및 개인정보 보유량에 따라 안전성 확보조치 적용 기준 차등

### Mail Security Solution

**SPAMSNIPER** - 스팸, APT 대응 메일보안

- 스팸(바이러스, 악성코드) 메일 차단(첨부파일 내)
- 실시간 스팸 패턴 분석 및 업데이트
- GS, CC, 조달청인증 획득 및 보안적합성검증 통과
- 가상화 기반 악성코드 분석 통합 이메일 APT 대응

**MAILSCREEN** - 메일DLP

- 메일 사전승인 후 외부전송
- 개인정보필터링(검출, 암호화)
- 첨부파일 압축, 암호화
- 권한/로그관리
- 비밀번호 변경 권고

**JVAULT+** - 메일 아카이빙

- 송수신메일 기록 보존(5년 이상), 위변조 방지, 로그 관리, 권한/접근 관리
- 개인정보 탐지 및 검출

### Document Security Solution

**OfficeHARD** - 보안파일서버

- 파일, 폴더, 전송구간 암호화, 보안
- 개인정보 필터링, 암호화
- 파일 송수신시 사전 결제
- 로그관리, 접근 통제, 권한 관리
- 비밀번호 연속오류시 사용제한
- 실시간 바이러스 검사, 차단
- KT 클라우드 플랫폼 기반 클라우드 서비스
- 개인정보 문서 탐지 및 중앙 서버 관리

**VEX** - 보안파일서버  
**CLOUD** - 보안파일서버 클라우드로  
**TAS** - 파일전송결재 시스템  
**PRIVACY** - 개인정보 문서중앙화

### Mobile Security Solution

**MOBILEKEEPER** - 모바일 단말관리

- 모바일 단말기 관리
- 모바일 APP 관리(카메라, 녹음, 화면캡처, Wi-Fi 등)
- 출입통제 차단

**MAM** - App보안 및 관리  
**MDAC** - 모바일 출입통제  
**SCREEN** - 모바일 화면캡처 차단

**MAILSAFER** - 모바일 이메일 보안

- 모바일 이메일에 대한 첨부파일 다운로드 통제 및 읽기전용(View Only)
- 메일 보내기 및 전달, 회신 등 주요 기능 통제
- 부서별/개인별 정책 설정 및 권한 부여
- 실시간 사용 현황 통계 관리

※ 법령 위계: 가이드라인 < 고시 < 시행규칙 < 시행령 < 법률

• 법률~고시: 법률 준수 및 시행을 위한 세부 사항(시행령~고시)으로 위반 시, 법적 구속력을 지님  
• 가이드라인: 법적 강제성은 없으나, 소관기관의 규정에 따라 법적 제재 효력 지님

IT 컴플라이언스 대응을 위한 JS 솔루션 가이드